What is claimed is:

1. A system for performing efficient computer virus scanning of transient messages using checksums in a distributed computing environment, comprising:

an antivirus system intercepting an incoming message at a network domain boundary, the incoming message including a body storing message content;

a parser module parsing the message content from the body and calculating a checksum over the parsed message content;

a checksum module storing the checksum in an information file associated with the incoming message in a transient message store;

an antivirus scanner scanning the incoming message for a presence of at least one of a computer virus and malware to identify infected message contents, and recording the checksum corresponding to each infected message content and an infection indicator.

2. A system according to Claim 1, further comprising:

a message queue enqueueing each incoming message and the associated information file.

3. A system according to Claim 1, further comprising:

a table of entries, each comprising the checksum and the infection indicator corresponding to each infected message content.

4. A system according to Claim 3, further comprising:

a comparison module comparing the checksum to the entries in the table prior to scanning operations, and discarding the incoming message if the checksum of the incoming message matches the checksum of one such entry with one such infection indicator.

5. A system according to Claim 3, further comprising:

a replacement module replacing entries in the table using a least-recently-used replacement algorithm.

6. A system according to Claim 3, wherein the table is structured as a binary tree.

7. A system according to Claim 1, wherein the checksum is calculated as a running checksum on a line-by-line basis as the incoming message is received.

8. A system according to Claim 1, wherein the message content further comprises at least one of an attachment and an embedded attachment.

9. A system according to Claim 1, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

10. A method for performing efficient computer virus scanning of transient messages using checksums in a distributed computing environment, comprising:

intercepting an incoming message at a network domain boundary, the incoming message including a body storing message content;

parsing the message content from the body and calculating a checksum over the parsed message content;

storing the checksum in an information file associated with the incoming message in a transient message store;

scanning the incoming message for a presence of at least one of a computer virus and malware to identify infected message contents; and

recording the checksum corresponding to each infected message content and an infection indicator.

11. A method according to Claim 10, further comprising:

enqueueing each incoming message and the associated information file onto a message queue.

12. A method according to Claim 10, further comprising:

maintaining a table of entries, each comprising the checksum and the infection indicator corresponding to each infected message content.

13. A method according to Claim 12, further comprising:

comparing the checksum to the entries in the table prior to scanning operations; and

discarding the incoming message if the checksum of the incoming message matches the checksum of one such entry with one such infection indicator.

14. A method according to Claim 12, further comprising:

replacing entries in the table using a least-recently-used replacement algorithm.

15. A method according to Claim 12, further comprising:

structuring the table as a binary tree.

16. A method according to Claim 10, further comprising:

calculating the checksum as a running checksum on a line-by-line basis as the incoming message is received.

17. A method according to Claim 10, wherein the message content further comprises at least one of an attachment and an embedded attachment.

18. A method according to Claim 10, wherein the distributed computing environment is TCP/IP-compliant and each incoming message is SMTP-compliant.

19. A computer-readable storage medium holding code for performing the method according to Claims 10, 11, 12, 13, 14, 15, 16, 17, or 18.

20. A system for performing efficient computer virus scanning of transient messages with message digests, comprising:

an antivirus system intercepting an incoming message at a network domain boundary, the incoming message including a header including fields, which each store field values, and a body storing message content;

a parser module parsing the field values from each field in the header and the message content from the body;

a digest module generating a message digest over each such field value and over the message content and recording the message digests corresponding to the incoming message;

an antivirus scanner scanning the incoming message for a presence of at least one of a computer virus and malware to identify infected message contents; and

an update module updating the message digest corresponding to each infected message content with an infection indicator.

21. A system according to Claim 20, further comprising:

a message queue enqueueing each incoming message.

22. A system according to Claim 20, further comprising:

a set of digests, each comprising the message digest and the infection indicator corresponding to each infected message content.

23. A system according to Claim 22, further comprising:

a comparison module comparing the message digest to the entries in the table prior to scanning operations, and discarding the incoming message if the message digest of the incoming message matches the message digest of one such entry with one such infection indicator.

24. A system according to Claim 20, wherein the message content further comprises at least one of an attachment and an embedded attachment.

25. A system according to Claim 20, wherein the message digest comprises at least one of SHA-1 and MD5 encryption.

26. A system according to Claim 20, wherein the bounded network domain is TCP/IP-compliant and each such message packet is SMTP-compliant.

27. A method for performing efficient computer virus scanning of transient messages with message digests, comprising:

intercepting an incoming message at a network domain boundary, the incoming message including a header including fields, which each store field values, and a body storing message content;

parsing the field values from each field in the header and the message content from the body and generating a message digest over each such field value and over the message content;

recording the message digests corresponding to the incoming message;

scanning the incoming message for a presence of at least one of a computer virus and malware to identify infected message contents; and

updating the message digest corresponding to each infected message content with an infection indicator.

28. A method according to Claim 27, further comprising:

enqueueing each incoming message onto a message queue.

29. A method according to Claim 27, further comprising:

maintaining a set of digests, each comprising the message digest and the infection indicator corresponding to each infected message content.

30. A method according to Claim 29, further comprising:

comparing the message digest to the entries in the table prior to scanning operations; and

discarding the incoming message if the message digest of the incoming message matches the message digest of one such entry with one such infection indicator.

31. A method according to Claim 27, wherein the message content further comprises at least one of an attachment and an embedded attachment.

32. A method according to Claim 27, wherein the message digest comprises at least one of SHA-1 and MD5 encryption.

33. A method according to Claim 27, wherein the bounded network domain is TCP/IP-compliant and each such message packet is SMTP-compliant.

34. A computer-readable storage medium holding code for performing the method according to Claims 27, 28, 29, 30, 31, 32, or 33.

35. A system for providing dynamic computer virus and malware protection of message packets in a bounded network domain, comprising:

an antivirus system intercepting an incoming message packet, each incoming message packet comprising a plurality of sections comprising a header storing field values and a body storing message packet content, and providing dynamic computer virus and malware protection, comprising at least one of:

a checksum module calculating and storing a checksum over the message packet content stored in the body of the incoming message packet; and

a digest module generating and storing a digest over at least one the field values stored in the header and the message packet content stored in the body of the incoming message packet;

an antivirus scanner scanning the incoming message packet if the at least one of the checksum and the digest have not been previously stored with an infection indicator indicating a presence of at least one of a computer virus and malware.

36. A system according to Claim 35, wherein the incoming message packet is discarded if the at least one of the checksum and the digest has been previously stored with an infection indicator indicating a presence of at least one of a computer virus and malware.

37. A system according to Claim 35, wherein the distributed computing environment is TCP/IP-compliant and each message packet is SMTP-compliant.

38. A method for providing dynamic computer virus and malware protection of message packets in a bounded network domain, comprising:

intercepting an incoming message packet, each incoming message packet comprising a plurality of sections comprising a header storing field values and a body storing message packet content;

providing dynamic computer virus and malware protection, comprising at least one of:

calculating a checksum over the message packet content stored in the body of the incoming message packet; and

generating a digest over at least one the field values stored in the header and the message packet content stored in the body of the incoming message packet;

storing at least one of the checksum and the digest; and

scanning the incoming message packet if the at least one of the checksum and the digest have not been previously stored with an infection indicator indicating a presence of at least one of a computer virus and malware.

39. A method according to Claim 38, further comprising:

discarding the incoming message packet if the at least one of the checksum and the digest has been previously stored with an infection indicator indicating a presence of at least one of a computer virus and malware.

40. A method according to Claim 38, wherein the distributed computing environment is TCP/IP-compliant and each message packet is SMTP-compliant.

41. A computer-readable storage medium holding code for performing the method according to Claims 38, 39, or 40.